MARTHA M. HALL
Attorney at Law
California State Bar No. 138012
964 Fifth Avenue, Suite 214
San Diego, California 92101
Telephone: (619) 544-1451
Facsimile: (619) 544-1473
E-mail: Martha_DiIorioHall@yahoo.com

Attorney for Defendant **Lowman**

UNITED STATES DISTRICT COURT

SOUTHERN DISTRICT OF CALIFORNIA

(HON. JOHN A. HOUSTON)

UNITED STATES OF AMERICA, Plaintiff, v. **TYLER LOWMAN, KARI LOWMAN, and MATTHEW HODLIN** Defendants.	Criminal No. 11-CR-3486-JAH-11 **REPLY TO GOVERNMENT'S RESPONSE AND OPPOSITION**

I.

SUPPLEMENTAL STATEMENT OF FACTS

The government is now maintaining that it searched the Terra Finance emails and digital data with the "consent" of Brian Peterson. What should first be noted is what is missing from the government's response, i.e. any evidence of Peterson's actual and specific consent to the search of the data within the possession of TecNique *prior* to the search.

The government presents two written and signed consent forms executed by Peterson on 1) July 23, 2009 and 2) September 9, 2009. Neither was a consent to search the back-up or data held by TecNique. The first consent signed on July 23, 2009 consented to the search the offices of Summit Lending located at 4120 Bonita

Road. The second consent, signed after Peterson had entered into his cooperation based plea agreement, was a consent to search a specific hard drive which had been seized by ICE. Government's Exhibits 1-A and 1-B, Doc. 777-1. Notably, in contrast to claims now being made that the plea agreement constituted some type of universal consent, the government sought and obtained a written consent form signed by Peterson on September 9, 2009 to search the hard drive which had been seized by ICE. This written consent to search the hard drive was signed over a month after he signed the cooperation agreement on July 31, 2009. Moreover, the government also sought and received a signed consent of Larry Stewart on November 23, 2009, even though that consent will not justify the search. These actions reveal that the government understood the law requires specific (preferably written) consent to search prior to the search to be sufficient to waive a Fourth Amendment right to be free of unreasonable searches and seizures.

Now, the government intends to rely on Mr Peterson's good word and his claim of his "intent" during 2009 when he was cooperating with the government to escape a lengthy prison sentence. Mr. Peterson is due to arrive in San Diego soon and it appears the government will be calling him to testify. However, the Court should be aware that Mr. Peterson, the owner of Terra Finance, sought to reduce his sentence by cooperating against his own employees. Mr. Peterson was responsible for the death of at least one individual when he crashed into the victim while driving drunk. Mr. Peterson has been convicted for domestic violence and other misdemeanors. Finally, Mr. Peterson's convictions and incarceration have not had much impact on him since while in jail he organized the purchase and importation of heroin into the jail, used some of the heroin and distributed some to others. The worst part, however, is that Mr. Peterson financed his jailhouse drug trade with funds from ***his mother*** which he obtained by telling his mother he needed the money for his legal defense. Mr. Peterson's credibility and "word" are therefore suspect.

II

ALL THOSE WHO COMMUNICATED VIA THE TERRA FINANCE EMAIL SERVER HAVE A REASONABLE AND LEGALLY RECOGNIZED EXPECTATION OF PRIVACY IN THOSE ELECTRONIC CONVERSATIONS THAT WAS VIOLATED BY THE GOVERNMENT'S SEARCH.

Government counsel begins with a citation to *United States v. Katz*, 389 U.S. 347 (1967) and defendants agree that *Katz* is the proper starting point. Indeed, *Katz* reveals some of the basic misconceptions and legal misunderstandings in the government's response. First, it should be noted that *Katz* was decided against the background of new technology – the ability to electronically eavesdrop on another's conversation. This new technology required a reassessment of the law governing searches to ensure that the new technology did not allow law enforcement to conduct and end-run around the protections of the Fourth Amendment.

In *Katz* the district court (the Southern District of California) and the Ninth Circuit Court of Appeals applied the then-current Fourth Amendment jurisprudence which required a trespass onto another's property to constitute a "search". The Supreme Court re-framed the question presented to take into account the realities of modern life:

> But this effort to decide whether or not a given "area," viewed in the abstract, is "constitutionally protected" deflects attention from the problem presented by this case. For the *Fourth Amendment* protects people, not places. What a person knowingly exposes to the public, even in his own home or office, [or on Facebook] is not a subject of *Fourth Amendment* protection. See *Lewis v. United States, 385 U.S. 206, 210*; *United States v. Lee, 274 U.S. 559, 563*. But what he seeks to preserve as private [on a password protected email account], even in an area accessible to the public, may be constitutionally protected. See *Rios v. United States, 364 U.S. 253*; *Ex parte Jackson, 96 U.S. 727, 733*.

Id., at 351-352. So too here the Fourth Amendment protects the people who were communicating via the Terra Finance email server. In fact, many of the email conversations were of a very private nature. Some defendants discussed marital problems via the email, others apologized for fights, still others discussed matters such a pregnancies and miscarriages. These are precisely the types of conversations that people intend to "preserve as private".

The Supreme Court has also held that "customary expectation of courtesy or deference [can provide] ... a foundation of *Fourth Amendment* rights." *Georgia v. Randolph*, 547 U.S. 103, 113 (2006), *citing Minnesota v. Olson*, 495 U.S. 91, 99 110 S. Ct. 1684 (1990) (holding that an overnight houseguest had a reasonable expectation of privacy in his belongings in friend's house). Applying the current customs and practices surrounding email conversations, it is clear that people expect a certain level of privacy in their email conversations.

There is no dispute that the law is evolving and attempting to catch up with the progress of technology. Thus, courts are struggling to provide the correct analytical framework to the new digital universe. However, contrary to the claims of the government, the cases demonstrate the courts' acceptance of a reasonable expectation of privacy in email communications.[1] There is a reasonable expectation of privacy in the stored electronic data and information contained in computers and smart phones

---

[1] In fact, the government cites many cases which actually hold that an employee retains a legitimate expectation of privacy in her or his computers. See, *Ziegler* and *Heckencamp*, *supra*. The government cites dicta from these cases and ignores the actual holdings to finesse its untenable position that the employees at Terra Finance had no expectation of privacy in their email. Gov't's R&O, Doc 775, page 11. Both held that persons have a legitimate expectation of privacy in digital information such as emails and computer files. *Sporer v. UAP Corp.,* No. C 08B02835 JSW, 2009 WL 2761329 (N.D. Cal. Aug 27, 2009) (unpublished) involved an employee suing his employer for wrongful termination when the employee was sending pornography over the company email. The Fourth Amendment is not mentioned once and this case is decided wholly under employment law precedent.

(which are small computers). *United States v. Warshak*, 631 F.3d 266, 288 (6th Cir.2010) (holding "that a subscriber enjoys a reasonable expectation of privacy in the contents of emails `that are stored with, or sent or received through, a commercial [internet service provider]' ") (citation omitted); *United States v. Finley*, 477 F.3d 250, 259 (5th Cir. 2007) (holding that defendant had a reasonable expectation of privacy in the text messages on his cell phone, and that he consequently had standing to challenge the search); see also, *United States v. Heckenkamp*, 482 F.3d 1142, 1146-47 (9th Cir. 2007) (holding that a student did not lose his reasonable expectation of privacy in information stored on his computer, despite a university policy that it could access his computer in limited circumstances while connected to the university's network); *United States v. Ziegler*, 474 F.3d 1184, 1189-90 (9th Cir. 2007) (holding that an employee had a reasonable expectation of privacy in a computer in a locked office despite a company policy that computer usage would be monitored); see also *In re Applications for Search Warrants for Information Associated with Target Email Address*, Nos. 12-MJ-8119-DJW & 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D.Kan. Sept.21, 2012) ("The Court finds the rationale set forth in *Warshak* persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received thorough an electronic communications service provider."); *United States v. Ali*, 870 F.Supp.2d 10, 39 n. 39 (D.D.C.2012) (" `We recognize individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider.' ") *quoting United States v. Lucas*, 640 F.3d 168, 178 (6th Cir.2011), in turn citing *Warshak*); *R.S. ex rel. S.S. v. Minnewaska Area School Dist*., No. 2149, 894 F.Supp.2d 1128, 1142 (D.Minn.2012) (holding "that one cannot distinguish a password-protected private Facebook message from other forms of private electronic correspondence," and thus, "based on established Fourth Amendment precedent, R.S. had a reasonable expectation of privacy to her

private Facebook information and messages"). The government's claims to the contrary are simply not supported by the law.

The government also tries to eviscerate this legally recognized expectation of privacy by arguing that emails are analogous to letters. However, email communications are far more similar to telephone conversations than to letters. Emails go back and forth, oftentimes rapidly. An email thread often reads like a conversation with questions and answers posed in short abbreviated sentences (oftentimes without punctuation). It is rare to see an email that reads like a letter. Indeed, the normal practice is to send formal letters as attachments to an email (just as the AUSA's practice in the instant case). Emails carry the same casual back-and-forth banter style of communication similar to telephone or even face-to-face conversations. Email correspondence is a digital conversation.

Therefore a more apt analogous framework is that provided in the context of wiretapped communications. As such, the seizure of an email thread is the legal equivalent of the tapping of a telephone call. Under the Title III, which "prohibits electronic surveillance by the federal government except under carefully defined circumstances," an "aggrieved person," as defined in 18 U.S.C. 2510 (11), possesses sufficient standing to move for suppression of evidence derived from electronic surveillance. 18 U.S.C. 2518(10)(a). An "aggrieved party" is a defined as a person who *was a party* to any intercepted wire, oral, or electronic communication, or a person against whom the interception was directed. 18 U.S.C. § 2510 (10, 11); see also, *Alderman v. United States,* 394 U.S. 165, 176-78 (1969) (holding that a defendant has standing to contest the use of evidence derived from eavesdropping if the defendant was a *party* to an intercepted conversation or "if the defendant himself was not intercepted," but he or she owned the premises upon which the interception had occurred); *see also United States v. Cella*, 568 F.2d 1266, 1280 (9th Cir. 1977) (citing *Alderman* and noting that any intercepted party has standing to challenge

lawfulness of wiretap); *United States v. Mercado*, 110 F. App'x 19, 21 (9th Cir. 2004) (a party has standing when his/her privacy has been invaded as a result of the wiretap). Thus any person who participated in an email communication or correspondence is an "aggrieved person" and has standing to contest the search.

Finally, contrary to the government's claims, individuals do not leave their Fourth Amendment rights at the door to their employment. The Supreme Court has repeatedly held that employee's possess reasonable expectations of privacy in certain areas of their work, even on work-provided computers, phones and pagers. *City of Ontario v. Quon*, 560 U.S. 747, 761, 130 S.Ct. 2619 (2010) and *O'Connor v. Ortega*, 480 U.S. 709, 725-26, 107 S.Ct. 1492 (1987). While, this expectation may be diminished when the employer needs to search the employees sphere for work-related reasons, that expectation of privacy is not forfeited for all purposes and certainly not forfeited for criminal investigations.

As noted above, here, it is obvious from a review of the emails that the employees of Terra Finance, like so many employees, were using their work email for both work and personal matters. Nor is this unusual or nefarious. As the *Quon* Court acknowledged, "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency." *Id.,* at 759, citing Amici brief.

Even resort to the words of the Fourth Amendment itself shows that the defendants here are in a position to invoke the protections of the Fourth Amendment. For, the first clause of the Fourth Amendment states that it protects "persons, houses, papers, and effects, against unreasonable searches and seizures . . . ." Today, a person's "papers and effects" are almost all stored on the computer, the email, the laptop and even the cell phone. These devices now hold our most treasured and closely guarded papers and effects – everything from the love letter to the will to the stock portfolio. For the Fourth Amendment to be relevant to our lives today, people

must have a legitimate and recognized expectation of privacy in their digital information.

III
THE GOVERNMENT HAS NOT AND CANNOT PROVE THAT BRIAN PETERSON GAVE SPECIFIC AND LEGALLY VALID CONSENT TO SEARCH THE BACK-UP DRIVE AND DIGITAL DATA STORED BY TECNIQUE *PRIOR* TO THAT SEARCH.

A. None of Peterson's Consents Provided by the Government Include a Consent to Search the Back-Up Drive Located at TecNique

In its opposition papers, the government cites to various consents that Peterson gave to search other items belonging to Terra. These consents are nothing more than red herrings because none of those consents include a consent to search the back-up drive located at TecNique.

1. The Written Consent to Search Peterson's Offices and Computers Found There are Limited in Scope and the Search at TecNique Was Beyond the Scope of Those Consents.

The government first relies on a written consent executed by Brian Peterson in July 2009 to search the Summit Lending offices at Claremont Mesa Blvd. and Bonita Road. See Gov't Opp., Exh. 1-A. In his declaration, Peterson characterizes this consent as covering a third office location, and states that he consented to a seizure of any documents, materials and items that the government sought at those three locations. Exh. 1-A, ¶ 3. The TecNique back-up, obtained from Larry Stewart in a parking garage in November 2009, was not obtained from any of these three locations and is not within the scope of this consent.

The government also relies on a second written consent executed by Brian Peterson in September 2009 to search an "image of hard drive seized by ICE." Gov't Opp., Exh. 1-C. In his declaration, Peterson states that this was a copy made of a hard drive from the Bonita Road location. Again, however, the TecNique back-up is not listed and is not within the scope of this consent.

The Fourth Amendment "requires that the scope of every authorized search be

particularly described." *Walter v. United States*, 447 U.S. 649, 657 (1980). Thus, even when a search is authorized by consent, "the scope of the search is limited by the terms of its authorization." *Shamaeizadeh v. Cunigan*, 338 F.3d 535, 547 (6th Cir. 2003), citing *Walter*, 447 U.S. at 656. It is a violation of the Fourth Amendment "for a consensual search to exceed the scope of the consent given." *United States v. Lopez-Cruz*, 730 F.3d 803, 809 (9th Cir. 2012). In measuring the scope of consent, a court must look to what "the typical reasonable person" would have understood by the exchange between the officer and the suspect. *Florida v. Jimeno*, 500 U.S. 248, 251 (1991). The standard does not turn on the subjective, unexpressed intent of the parties, but is rather a test of objective reasonableness. See *Lopez-Cruz*, 730 F.3d at 809.

In *Lopez-Cruz,* for example, a suspect consented to border patrol agents "look[ing] in" and "search[ing]" the cellular telephones in his vehicle. See 730 F.3d at 806. When one of the telephones rang, the agent answered the incoming call and impersonated the intended recipient. See *id*. On review, the Ninth Circuit found that the agent had exceeded the scope of the consent given. See *id*. at 810. In particular, the court held that even if the agent had consent to manipulate the phone to search the contents and read text messages, answering an incoming call constituted a meaningful difference in the method and scope of the search. See *id*. The court further noted that, although answering incoming calls would have fell within the scope of a search warrant, "a search warrant is materially different from consent." *Id*. at 810. Whereas a search pursuant to a warrant is limited by the extent of the probable cause supporting the issuance of the warrant, "a search pursuant to consent is limited by the extent of the consent given for the search by the individual." *Id*. at 810. Because the agent did not have a warrant, "he did not have authority to search for evidence that might have fallen within the scope of a warrant that he did not have." *Id*. at 810.

Here, likewise, the government failed to get a warrant to search the hard drive

located at TecNique. It therefore cannot rely on an expanded or open-ended definition of the property to be searched, such as it might have sought in the hypothetical warrant that it did not in fact obtain. Rather, the government is limited to the specific, circumscribed scope of the consents it actually obtained from Peterson. Whatever the validity of these written consents, they cannot be reasonably and objectively construed as covering the TecNique back-up. The consents are circumscribed in scope to cover specific property and/or property obtained from specific locations. The TecNique back-up is not listed on either of the consents, nor was it obtained at any of the three office locations. Rather, Larry Stewart of TecNique had made a back-up of Terra Finance's server nearly two years prior, in late 2007 or early 2008, when Terra Finance had ceased operations. TecNique's back-up is plainly beyond the scope of these written consents.

2. The Cooperation Agreement Provision to Provide Documents is Not and Does Not Purport to Be a Consent Which Waives Fourth Amendment Protections

The government next relies on a Cooperation Addendum executed by Peterson in July 2009, in which he agreed to "produce all documents and other evidence in [his] possession or control" relating to certain federal crimes. Gov't Opp., Exh. 1-B. Again, however, this document cannot support a search of the TecNique hard drive.

The Cooperation Addendum includes promises by Peterson to cooperate prospectively with the government in its investigation in return for possible leniency. It does not itself constitute any specific act of cooperation. Indeed, the addendum contemplates Peterson's possible refusal to cooperate in the future, and sets forth the consequences of such a breach.

Moreover, the Addendum cannot reasonably and objectively be construed as a consent to search. The Addendum does not identify or discuss any Fourth Amendment protections, much less purport to waive those protections held by Terra Finance or its employees and contractors. The Addendum does not specify any

obligations of Peterson as a fiduciary for Terra Finance, as opposed to his obligations individually. The Addendum does not specify a consent to search any specific property, much less identify the TecNique back-up obtained from a third party months later. Finally, the government's actions in obtaining a consent to search a particular hard drive from Peterson more than a month after he signed the cooperation agreement indicates an understanding that the cooperation agreement could not constitute consent sufficient to waive Fourth Amendment rights.

Because the Addendum does not include a consent to any search, much less particularly describe the TecNique hard drive, it cannot justify the search of that material. See generally, *Walter,* 447 U.S. 649; *Shaibu*, 920 F.2d 1423; and *United States v. Lopez,* 730 F.3d 803 (all cited and discussed *supra*).

B. An "Intent to Consent" Does Not Constitute Consent Under the Fourth Amendment

Having chosen to obtain the private, sensitive electronic communications of Terra Finance employees and contractors without a warrant, the government now tries to rely on the purported consent of Brian Peterson in 2009. Because the government never obtained consent to search TecNique's back-up from Peterson, it presents and relies upon Peterson's other consents: 1) the written consent to search the offices of Summit Lending located on 4120 Bonita Road signed on July 23, 2009; 2) the written consent to search the hard drive seized by ICE signed on September 9, 2009 and finally, 3) the purported universal consent the government derives from the cooperation plea agreement signed by Peterson on July 31, 2009. Government Exhibits 1-A through 1-C, Doc 777-1. At the time of these purported consents, Terra Finance was "effectively closed," Gov't Opp. Exh. 1-A, ¶ 2, and Peterson had executed a plea agreement and cooperation addendum in the hopes of obtaining leniency despite his own admitted felony criminal conduct. Peterson was therefore no longer acting in his capacity as an employer or exercising his fiduciary duties to the company in deciding to cooperate with the authorities for his own benefit. But even

assuming that Peterson had the authority to give legally valid consent, a close reading of the government's papers show that he did not, in fact, consent to the search of the hard drive obtained from TecNique.

When a prosecutor seeks to rely upon consent to justify a warrantless search, the government "always bears the burden of proof to establish the existence of effective consent." *United States v. Shaibu,* 920 F.2d 1423, 1426 (9th Cir. 1990) (internal quotations and citations omitted); accord *Bumper v. North Carolina*, 391 U.S. 543 (1968). Moreover, the "existence of consent to a search is not lightly to be inferred." *Shaibu*, 920 F.2d at 1426 (internal quotations and citations omitted). The government's burden is not met by a showing of "no more than acquiescence," *Bumper*, 391 U.S. at 548-49, or by a "failure to object," *Shaibu*, 920 F.2d at 1427. To do so would impermissibly shift the burden away from the government to show "unequivocal and specific consent." *Shaibu*, 920 F.2d at 1427-28.

Here, the government has not shown the necessary unequivocal and specific consent to search the hard drive possessed by TecNique. As discussed in the moving papers, the government obtained that hard drive from Larry Stewart during a parking garage meeting. The government further had Stewart repeatedly execute detailed and specific consent forms for the search of that hard drive, which contained the confidential data of not only Terra Finance but also Prudential of California, despite Stewart's lack of authority to authorize such a search. No such consent forms were executed by Peterson for the search of the TecNique hard drive. Neither does Peterson's self-serving declaration, executed more than four years after the search, anywhere state that he gave specific verbal consent to search that hard drive. Rather, years after seizure of the hard drive and only after defense counsel in this case raised concerns about the search, government agents returned to Stewart in an attempt to rely on a theory of abandonment, which Stewart would not support. See Defense Motion, Exh. C.

Whether the government now regrets that it failed to obtain Peterson's consent to the search, or whether Peterson might have consented had he been asked at the time, is irrelevant to the validity of the search at the time. Even where an employer has the ability to consent to a search, "[t]he remaining question is ... did it consent to a search." *United States v. Ziegler*, 474 F.3d 1184, 1192 (9th Cir. 2007). Here, Peterson did not. The fact that the government had Peterson execute a second written consent form ***after*** the purported universal consent in his cooperation agreement further proves that the government was aware that the cooperation agreement was not valid consent to search. Also, the fact that the government obtained a second signed consent and listed with specificity the item to be searched in that consent demonstrates that in 2009 the government understood what was required by the Fourth Amendment, i.e. specific, clear consent to search a particular place or a specific thing. Such consent to search the back-up from TecNique was never obtained from Peterson.

To the extent that the government is now trying to obtain retroactive consent to an earlier search, that effort must also fail. It is long settled that "[a] search conducted in reliance upon a warrant cannot later be justified on the basis of consent if it turns out that the warrant was invalid. The result can be no different when it turns out that the State does not even attempt to rely upon the validity of the warrant, or fails to show that there was, in fact, any warrant at all." *Bumper*, 391 U.S. at 549-50. Because the government has not shown a specific, legally valid consent to the search of the TecNique hard drive, all evidence on that hard drive as well as the fruits of that evidence should be suppressed.

//

//

//

//

IV

THE EMPLOYEE BOILERPLATE CONTRACT DOES NOT AMOUNT TO A KNOWING AND VOLUNTARILY WAIVER OF FOURTH AMENDMENT RIGHTS

Finally, the government relies on a Terra Finance "Policies and Procedures" manual to argue that employees had no reasonable expectation of privacy in their e-mails. See Gov't Opp. Exh. 1-D. But the boilerplate language in that manual, which was never enforced at Terra Finance, does not amount to a knowing and voluntary waiver of Fourth Amendment rights.

As discussed above, employees have a reasonable expectation of privacy against intrusions by police, even within the workplace context. See *O'Connor v. Ortega*, 480 U.S. 709, 716 (1987). "As with the expectation of privacy in one's home, such an expectation in one's place of work is 'based upon societal expectations that have deep roots in the history of the [Fourth] Amendment.'" *Id.* at 716 (citation omitted). Moreover, as the Supreme Court recently noted, the courts must "proceed with care when considering the whole concept of privacy expectations in communications made on electronic equipment owned by a government employer." *Ontario v. Quon*, 560 U.S. 746, 759 (2010). That is because not only the technology itself, but societal norms of proper behavior in relation to that technology, are rapidly changing. See *id*. at 759. Thus, "many employers expect or at least tolerate personal use of such equipment by employees because it often increases worker efficiency." *Id*. at 759.

"Under the approach of the *O'Connor* plurality, when conducted for a 'noninvestigatory, work-related purpos[e]' or for the 'investigatio[n] of work-related misconduct,' a government employer's warrantless search is reasonable if it is ""justified at its inception"" and if ""the measures adopted are reasonably related to the objectives of the search and not excessively intrusive in light of"" the circumstances giving rise to the search." *Quon*, at 761, *quoting O'Connor*, 480 U.S.,

at 725-726, 107 S. Ct. 1492; see also, *United States v. Jones*, 286 F.3d 1146, 1151 (9th Cir. 2002)("a public employer 'cannot cloak itself in its public employer robes in order to avoid the probable cause requirement when it is acquiring evidence for a criminal prosecution.'") (*quoting United States v. Taketa*, 923 F.2d 665,675 (9th Cir. 1991)).

In fact, the ***reason*** the Supreme Court upheld the search of the employee's pager texts in *Quon* was precisely because it was for a legitimate work-related reason and not for any investigatory purpose. The Court began it's analysis stating, "[f]or present purposes we assume several propositions, *arguendo:* First, Quon had a reasonable expectation of privacy in the text messages sent on the pager provided to him by the City; second, petitioners' review of the transcript constituted a search within the meaning of the *Fourth Amendment*; and third, the principles applicable to a government employer's search of an employee's physical office apply with at least the same force when the employer intrudes on the employee's privacy in the electronic sphere." *City of Ontario, California v. Quon*, 560 U.S. 746, 760, 130 S.Ct. 2619 (2010).

Perhaps the most important aspect of *Quon* for the present case is that there was an "employee" contract there similar to the contract upon which the government relies here. The contract in *Quon* "specified that the City 'reserves the right to monitor and log all network activity including e-mail and Internet use, with or without notice. Users should have no expectation of privacy or confidentiality when using these resources.'" *Id.,* at 751. Yet, this contract was practically irrelevant to the Supreme Court. What was relevant was the purpose behind the initiation of the search: was it a legitimate work-related search or was it an investigatory search. A fair reading of both *Quon* and *O'Connor* leads, ineluctably, to the conclusion that the search of the Terra Finance back-up files at TecNique fell outside the employer-employee exception. See also, *United Sates v. Taketa*, 923 F.2d 664, 672 (9th Cir.

1991) (holding that company regulation requiring employees to maintain clean desks could not "reasonably serve as an after-the-face rationalization" for a search of a desk when the regulation was never enforced by a routine or regular practice of inspections.)

The Ninth Circuit has held, in a case preceding *Quon*, that an employee's subjective expectation of privacy at work may be diminished by an employment regulation, even if that expectation is otherwise objectively reasonable. *United States v. Ziegler*, 474 F.3d 1184 (9th Cir. 2007). To the extent that *Ziegler* upholds an employer search initiated for law-enforcement purposes or criminal investigation, it has been overruled by *Quon*. Even if *Ziegler* is still good law, it is distinguishable from the present case in significant ways. In *Ziegler*, the Ninth Circuit addressed a government search of an employee's office computer. In that case, the company employees had been advised in an employment manual and through training that their internet activities were being monitored and should not be used for activities of a personal nature. See *id*. at 1192. But the Ninth Circuit's inquiry did not end there. Rather, the court also looked to the actual practice of the company, which included routine and often daily monitoring of internet traffic through its computers. See *id*. at 1191-92. Only after considering both the company's regulations and its actual practices did the Ninth Circuit uphold the employer's ability to consent to a search of an employee's computers. See *id*. at 1192.

Here, unlike in *Ziegler*, the purported policies set forth in Terra Finance's employee manual were never actually enforced. Although the manual specified that e-mail should be used for business purposes only, that provision was widely ignored, with employees using e-mails to discuss jokes, leisure activities, and highly personal matters such as marital conflicts, pregnancies, and miscarriages. Although the manual warned that Terra had the capability of monitoring and tracking internet and e-mail activities, there has been no showing that any such monitoring or tracking was

actually done. Finally, the manual specified that violation of its computer policies would result in disciplinary action, up to and including termination, see Exh. 1-D at p.13, but there has been no showing that such action ever occurred. Accordingly, the unenforced and widely ignored provisions of the manual on computer use did not alter the employees' reasonable expectation of privacy in their e-mails.

Equally important, the boilerplate provisions in the manual did not constitute a knowing and voluntary waiver of Fourth Amendment rights. Non-employees of Terra Finance, such as contractors and others who exchanged e-mails captured by the Terra server, were not even signatories to the manual. Employees were required to sign the manual at the outset of employment, with no opportunity to refuse or negotiate any of the provisions. Rather, the manual was drafted by the employer and offered as a contract of adhesion, with no bargaining power on the side of the employee. Finally, the manual nowhere discusses employees' Fourth Amendment rights. Accordingly, it cannot constitute a knowing and voluntary waiver of the Fourth Amendment or privacy rights of employees and contractors in their electronic communications.

Even if Terra Finance employees consented to some intrusion into their workplace activities by their employer, that consent could not justify a government search of their electronic communications years after those communications occurred and after the company ceased operations. As the Ninth Circuit has noted, "operational realities of the workplace" may defeat an employee's expectation of privacy "when an intrusion is by a supervisor rather than a law enforcement official." *Taketa*, 923 F.2d at 673. But "an employee's assent [to search] is merely a relevant factor in determining how strong his expectation of privacy is." *United States v. Scott*, 450 F.3d 863, 868 (9th Cir. 2006). Even if that consent might reduce a defendant's expectation of privacy, it is only valid if the search is otherwise reasonable. See 450 F.3d at 868, 871. Here, unenforced and boilerplate regulations about a company's right to monitor computer activities could not reasonably be

construed to authorize a government search of back-up data held by the company's internet service provider. The company manual therefore cannot justify the government's warrantless search.

V.

CONCLUSION

The defendants recognize the superficial appeal of the government's reliance of Peterson's "intent to consent". Peterson, after all, did consent to several searches and agreed to cooperate in any and all ways with the government. However, the argument that the government ***could have*** obtained the necessary and specific consent to search the back-up located at TecNique is no more legitimate that the government's oft-repeated claim that it could have obtained a warrant since probable cause existed. *Katz*, at 356-57 ("this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful 'notwithstanding facts unquestionably showing probable cause,' *Agnello v. United States, 269 U.S. 20, 33*, for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . .").

//

//

//

//

//

//

//

//

//

So too, the government's failure to obtain the consent required is not some technicality that should be dispensed with because *they could have done it right*. Rather, the failure to obtain either the necessary warrant or the required consent goes to the heart of the Fourth Amendment. This Court is charged with protecting those rights guaranteed by the Fourth Amendment. To do so, the data retrieved from the back-up kept and held by TecNique for Terra Finance must be suppressed.

Respectfully submitted,

Dated: April 23, 2014

S/Martha M. Hall
MARTHA M. HALL
Attorney at Law
Attorney for Defendant **Tyler Lowman**

Dated: April 23, 2014

S/Jennifer Coon
JENNIFER COON
Attorney at Law
Attorney for Defendant **Kari Lowman**

Dated: April 23, 2014

S/Gerard Wasson
GERARD WASSON
Attorney at Law
Attorney for Defendant **Hodlin**